CLAIMS

What is claimed is:

1. An overlay network for maintaining traffic flow between a client and a server during a denial of service attack, comprising:

a set of overlay nodes, coupled between the client and the server, wherein each overlay node comprises:

a ranking module configured to rank the overlay nodes based on a performance metric, wherein an overlay node with a higher-ranking indicates that the overlay node has better performance for transferring traffic to the server than overlay nodes with lower-rankings; and

a probing module configured to probe a portion of the overlay nodes with higher-rankings more frequently than overlay nodes with lower-rankings during probing intervals.

2. The overlay network as recited in Claim 1, wherein each overlay node further comprises a path selection module, configured to dynamically select an overlay node with a highest-rankings to be included as part of a pathway for transferring traffic to the server.

3. The overlay network as recited in Claim 1, further comprising an access node, configured to authenticate traffic directed to the server from the client, and forward authenticated traffic to one or more of the overlay nodes.

4. The overlay network as recited in Claim 1, further comprising one or more target nodes, configured to transfer the traffic from one or more of the

overlay nodes directly to the server, the one or more target nodes having exclusive knowledge of an identity for the server.

5. The overlay network as recited in Claim 1, wherein each overlay node is virtually connected to each other.

6. The overlay network as recited in Claim 1, wherein the performance metric includes at least one of: available bandwidth, latency, loss rate, and jitter; and wherein an overlay node with a higher-ranking indicates that the overlay node has better performance for transferring traffic to the server than overlay nodes with lower-rankings, the better performance including at least one of: more available bandwidth, less jitter, lower latency, and less packet loss.

7. The overlay network as recited in Claim 1, wherein the ranking module is further configured to determine whether the portion of overlay nodes with higher-rankings continue to have better performance for transferring traffic to the server than one or more of the overlay nodes with lower-rankings after a probing interval.

8. The overlay network as recited in Claim 1, wherein the ranking module is configured to demote the rankings of the portion of overlay nodes with higher-rankings to lower-rankings if the portion of overlay nodes with higher-rankings have worse performance for transferring traffic to the server than one or more of the overlay nodes with lower-rankings after a probing interval.

9. The overlay network as recited in Claim 1, wherein the traffic is data.

10. A method for evaluating overlay nodes in a network to mitigate against a denial of service attack, the method comprising:

ranking the overlay nodes based on a performance metric, wherein an overlay node with a higher-ranking indicates that the overlay node has better performance for transferring traffic to a target than overlay nodes with lower-rankings; and

probing a portion of the overlay nodes with higher-rankings more frequently than overlay nodes with lower-rankings during probing intervals.

11. The method as recited in Claim 10, wherein the performance metric includes at least one of: available bandwidth, latency, loss rate, and jitter.

12. The method as recited in Claim 10, wherein an overlay node with a higher-ranking indicates that the overlay node has better performance for transferring traffic to a target than overlay nodes with lower-rankings, the better performance including at least one of: more available bandwidth, less jitter, lower latency, and less packet loss.

13. The method as recited in Claim 10, wherein the portion of the overlay nodes with higher-rankings includes one or more overlay nodes.

14. The method as recited in Claim 10, wherein the target includes at least one of: an overlay node, an overlay node with exclusive access to a host server, and a host server.

15. The method as recited in Claim 10, further comprising determining whether the portion of overlay nodes with higher-rankings continue to have better performance for transferring traffic to a target than one or more of the overlay nodes with lower-rankings after a probing interval.

16. The method as recited in Claim 10, further comprising determining whether the portion of overlay nodes with higher-rankings continue to have better performance for transferring traffic to a target than one or more of the overlay nodes with lower-rankings after a probing interval; and

demoting the rankings of the portion of overlay nodes with higher-rankings to lower-rankings if the portion of overlay nodes with higher-rankings have worse performance for transferring traffic to a target than one or more of the overlay nodes with lower-rankings.

17. The method as recited in Claim 10, further comprising determining whether the portion of overlay nodes with higher-rankings continue to have better performance for transferring traffic to a target than one or more of the overlay nodes with lower-rankings after a probing interval; and

promoting the rankings of one or more of the overlay nodes with lower-rankings to higher-rankings, if the portion of overlay nodes with higher-rankings have worse performance for transferring traffic to a target than one or more of the overlay nodes with lower-rankings.

18. The method as recited in Claim 10, further comprising selecting the portion of the overlay nodes with higher-rankings to be included as part of a pathway for transferring traffic to a target.

19. One or more computer-readable media comprising computer executable instructions that, when executed, direct a computer to:

evaluate overlay nodes in an overlay network;

rank the overlay nodes based on a performance metric, wherein an overlay node with a higher-ranking indicates that the overlay node has better performance for transferring traffic to a target than overlay nodes with lower-rankings; and

probe a portion of the overlay nodes with higher-rankings more frequently than overlay nodes with lower-rankings during probing intervals.

20. One or more computer-readable media as recited in Claim 19, further comprising computer executable instructions that, when executed, direct the computer to: determine whether the portion of overlay nodes with higher-rankings continue to have better performance for transferring traffic to a target than one or more of the overlay nodes with lower-rankings after a probing interval.

21. One or more computer-readable media as recited in Claim 19, further comprising computer executable instructions that, when executed, direct the computer to: determine whether the portion of overlay nodes with higher-rankings continue to have better performance for transferring traffic to a target than one or more of the overlay nodes with lower-rankings after a probing interval; and

demote the rankings of the portion of overlay nodes with higher-rankings to lower-rankings if the portion of overlay nodes with higher-rankings have worse performance for transferring traffic to a target than one or more of the overlay nodes with lower-rankings.

22. In a network comprising overlay nodes interspersed between a server and client, a system for mitigating against a denial of service attack, the system comprising:

means for probing overlay nodes in the network during a probing interval to determine connectivity levels of each overlay node;

means for ranking each overlay node wherein an overlay node having a highest-ranking has a highest connectivity potential for transferring traffic to the server;

means for selecting the overlay node with the highest-ranking to be included as part of a pathway for transferring the traffic to the server; and

means for probing a portion of the overlay nodes with higher-rankings more frequently than other overlay nodes during subsequent probing intervals.

23. An overlay network to mitigate a Denial of Service attack, comprising:

access nodes configured to authenticate traffic directed to a server from a client;

target nodes configured to transfer the traffic previously authenticated by the access nodes to the server; and

overlay nodes, coupled between the access nodes and the target nodes, configured to route the traffic from the access nodes to the target nodes by selecting a best end-to-end path between the client and the server based in accordance with at least one performance metric.

24. The overlay network as recited in Claim 23, wherein each overlay node is configured to dynamically select, a best target node for accessing the server and a best path to reach that target node.

25. The overlay network as recited in Claim 24, wherein the best path is selected via a best next hop measured in terms of the at least one performance metric.

26. The overlay network as recited in Claim 23, wherein each overlay node comprises:

a ranking module configured to rank the overlay nodes based on the performance metric, wherein an overlay node with a higher-ranking indicates that the overlay node has better performance for transferring traffic to one of the target nodes than overlay nodes with lower-rankings; and

a probing module configured to probe a portion of the overlay nodes with higher-rankings more frequently than overlay nodes with lower-rankings during probing intervals.

27. In an overlay network, a node for maintaining traffic flow between a client and a server during a denial of service attack, the node comprising:

a ranking module configured to rank overlay nodes coupled between the client and the server based on a performance metric, wherein overlay nodes with a higher-ranking indicates that the overlay nodes have better performance for transferring traffic to the server than overlay nodes with lower-rankings; and

a probing module configured to probe a portion of the overlay nodes with higher-rankings more frequently than overlay nodes with lower-rankings during probing intervals.